

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Kiyoshi KOHIYAMA et al.

Application No.: Unassigned

Group Art Unit: Unassigned

Filed: July 30, 2003

Examiner: Unassigned

For: METHOD OF AND APPARATUS FOR REPRODUCING INFORMATION, AND
SECURITY MODULE

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2002-221856

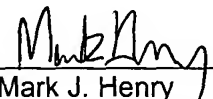
Filed: July 30, 2002

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 30, 2003

By: 
Mark J. Henry
Registration No. 36,162

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月30日

出 願 番 号

Application Number:

特願2002-221856

[ST.10/C]:

[JP2002-221856]

出 願 人

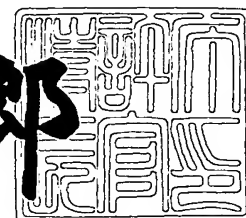
Applicant(s):

富士通株式会社

2003年 1月10日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2002-3105058



【書類名】 特許願

【整理番号】 0252043

【提出日】 平成14年 7月30日

【あて先】 特許庁長官殿

【国際特許分類】 G07B 15/00

【発明の名称】 情報再生装置および情報再生方法

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小桧山 清之

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 吉武 敏幸

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 渡部 康弘

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 森岡 清訓

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100089118

 【弁理士】



【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【その他】 国等の委託研究の成果に係る特許出願（平成14年度通信・放送機構「PCなどオープンアーキテクチャデジタル放送受信機に対応する権利保護システムの研究開発」委託研究、産業活力再生特別措置法第30条の適用を受けるもの）

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【ブルーフの要否】 要



【書類名】 明細書

【発明の名称】 情報再生装置および情報再生方法

【特許請求の範囲】

【請求項 1】 情報を再生する情報再生装置において、

内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、

外部から参照することが可能なメモリと、

前記セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスにより前記メモリに格納されたメモリ格納情報を読み出し、該メモリ格納情報と、前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック手段と、

を備えたことを特徴とする情報再生装置。

【請求項 2】 前記セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスにより前記メモリに格納されたメモリ格納情報を書き換える書き換え手段を備え、前記改ざんチェック手段は、書き換え後のメモリ格納情報と前記セキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックすることを特徴とする請求項 1 に記載の情報再生装置。

【請求項 3】 前記セキュアモジュールに実装され、原情報に変更をかけ、変更後の情報をメモリ格納情報として前記メモリに格納する格納制御手段を備えたことを特徴とする請求項 1 または 2 に記載の情報再生装置。

【請求項 4】 前記格納制御手段は、前記メモリ格納情報を更新した場合に、更新前のメモリ格納情報から更新後のメモリ格納情報への引継を行わせることを特徴とする請求項 3 に記載の情報再生装置。

【請求項 5】 前記格納制御手段は、前記セキュアモジュール内のみに存在する鍵を用いて前記原情報を暗号化し、暗号化された原情報を前記メモリ格納情報として前記メモリに格納することを特徴とする請求項 3 または 4 に記載の情報再生装置。

【請求項 6】 前記セキュアモジュールに実装されており、前記メモリ格納

情報の暗号化または復号化に用いられる鍵を保持し、前記改ざんチェック手段により改ざんが検知されない場合、鍵を外部へ供給する鍵管理手段を備えたことを特徴とする請求項 1 ～ 5 のいずれか一つに記載の情報再生装置。

【請求項 7】 前記鍵管理手段は、前記改ざんチェック手段により改ざんが検知された場合、前記鍵の供給を停止することを特徴とする請求項 6 に記載の情報再生装置。

【請求項 8】 前記セキュアモジュールに実装され、直接アクセスにより、前記セキュアモジュール内の秘密情報を前記メモリに書き込む書込手段を備え、前記改ざんチェック手段は、書き込まれた前記秘密情報に対応する応答情報に基づいて前記メモリ格納情報の改ざんをチェックすることを特徴とする請求項 1 ～ 7 のいずれか一つに記載の情報再生装置。

【請求項 9】 前記秘密情報は、1 度目で正規の情報が読み出され 2 度目で違う情報が読み出されるように制御されるメモリ空間に格納されていることを特徴とする請求項 8 に記載の情報再生装置。

【請求項 10】 内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュール内で実行され、いずれの手段も介さずに直接アクセスにより外部から参照することが可能なメモリに格納されたメモリ格納情報を読み出す読み出し工程と、

読み出された前記メモリ格納情報と前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック工程と、

を備えたことを特徴とする情報再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば、インターネットを介してダウンロードされた情報または記録媒体に格納されている情報を再生するための情報再生装置および情報再生方法に関するものであり、特に、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェアを付加することで、安全なソフ

トウェア処理を実行することができる情報再生装置および情報再生方法に関するものである。

【0002】

【従来の技術】

近年、ブロードバンドインターネットやデジタル放送が普及しつつあり、配信されたコンテンツ（主に、デジタルAV（Audio Video）の安全性を保障する権利保護技術がクローズアップされている。

【0003】

この中でも特にパーソナルコンピュータ（PC：Personal Computer）は、オープンアーキテクチャであり、基本的に覗き見が出来るため、安全性の実現が困難とされている。

【0004】

しかしながら、一方でパーソナルコンピュータは、ブロードバンドインターネットの主要な出入り口として機能している。従って、パーソナルコンピュータ（出入り口）で安全性が保障される場合には、インターネット全体でのデジタルAVコンテンツの配信が可能になり意義が大きい。

【0005】

従来より、パーソナルコンピュータのソフトウェアによる権利保護については、安全性を保障するアルゴリズムの解析を困難にする難読化による手法が主流であった。

【0006】

しかしながら、パーソナルコンピュータ上のソフトウェアにおいては、一旦、メインメモリ上に実装してしまえば、コピーすることが容易であり、コピーした結果を時間をかけて解析することで、権利保護アルゴリズムが解析できる。

【0007】

従って、難読化による権利保護のシステムは、安全性が低いシステムであると考えられ、放送等恒常性が高いシステムで一度解析されたことによる被害を想定すると、採用が困難である。

【0008】

図 7 は、パーソナルコンピュータ 5 0 を用いた従来のシステムの構成例を示すブロック図である。この図に示したように、従来のシステムは、パーソナルコンピュータ 5 0、ネットワーク 5 1、スピーカ 5 2、表示装置 5 3 および入力装置 5 4 によって構成されている。

【 0 0 0 9 】

パーソナルコンピュータ 5 0 は、情報再生装置としての機能を備えており、CPU (Central Processing Unit) 5 0 a、ROM (Read Only Memory) 5 0 b、RAM (Random Access Memory) 5 0 c、ハードディスクドライブ 5 0 d、MB (Multimedia Board) 5 0 e、I/F (Interface) 5 0 f、I/F 5 0 g、バス 5 0 h によって構成され、ネットワーク 5 1 を介してダウンロードされた暗号化情報やハードディスクドライブ 5 0 d に格納された暗号化情報を復号してスピーカ 5 2 および表示装置 5 3 へ出力する。

【 0 0 1 0 】

CPU 5 0 a は、ハードディスクドライブ 5 0 d に格納されているプログラムに従って各種演算処理を実行するとともに、装置の各部を制御する。ROM 5 0 b は、CPU 5 0 a が実行する基本的なプログラムやデータを格納している。RAM 5 0 c は、CPU 5 0 a が各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。

【 0 0 1 1 】

ハードディスクドライブ 5 0 d は、CPU 5 0 a が実行するプログラムやデータ等を格納している。MB 5 0 e は、CPU 5 0 a から供給され、暗号化された音声データや画像データを復号し、元の音声信号や画像信号を生成した後、これらをスピーカ 5 2 および表示装置 5 3 へ出力する。

【 0 0 1 2 】

I/F 5 0 f は、ネットワーク 5 1 を介して情報を送受信する際のインタフェースであり、プロトコル変換やデータのフォーマット変換を実行する。I/F 5 0 g は、入力装置 5 4 より入力されたデータを、パーソナルコンピュータ 5 0 の内部形式のデータに変換する。

【 0 0 1 3 】

バス50hは、CPU50a、ROM50b、RAM50c、ハードディスクドライブ50d、MB50e、I/F50fおよびI/F50gを相互に接続し、これらの間で情報の授受を可能にする。

【0014】

ネットワーク51は、例えば、インターネットにより構成されている。スピーカ52は、MB50eから供給された音声信号を音声に変換して出力する。表示装置53は、例えば、CRT (Cathode Ray Tube) モニタや液晶モニタによって構成されており、MB50eから供給された画像信号を画像として表示する。入力装置54は、例えば、マウスやキーボードによって構成されている。

【0015】

図8は、図7に示したパーソナルコンピュータ50における情報の流れを示す図である。同図に示したように、ハードディスクドライブ50dには、基本ソフトウェア、暗号解読鍵群および暗号化コンテンツが格納されている。

【0016】

ここで、基本ソフトウェアは、暗号化コンテンツの暗号を解読するための処理を等を行うためのソフトウェアであり、悪意あるユーザに解読されるのを防止することを目的として、難読化されている。この難読化とは、以下のような処理が施されていることをいう。

【0017】

難読化前 $X = X + Y$

難読化後 $X = X * 2 + 1 + Y * 2 - 1$

$X = X + 2$

【0018】

すなわち、上記のように、難読化の前後で演算結果が同じであるが、難読化後は、アルゴリズムを解読するのが難しくなっている。

【0019】

ハードディスクドライブ50dにおける暗号解読鍵群は、暗号化コンテンツに施されている暗号を解読するための複数の鍵であり、悪意あるユーザに容易に取得されないようにすることを目的として、秘密のスクランブルが施された状態で

秘密の場所に格納されている。

【 0 0 2 0 】

暗号化コンテンツは、暗号化処理が施されたコンテンツであり、例えば、画像、音声、コンピュータデータ等から構成されている。

【 0 0 2 1 】

暗号化コンテンツの再生が開始されると、以下の処理が実行される。

(1) ハードディスクドライブ 5 0 d から難読化された基本ソフトウェアが読み出され、RAM 5 0 c 上に実装される。

【 0 0 2 2 】

(2) 読み出された基本ソフトウェアは、必要に応じて秘密の場所に格納され、秘密のスクランブルがかかった暗号解読鍵がハードディスクドライブ 5 0 d から読み出される。暗号解読鍵は、例えば、3 ～ 5 箇所に分けて秘密の場所に格納され、秘密の演算等を施さないと目的の鍵が得られないように処理されている。

【 0 0 2 3 】

(3) ハードディスクドライブ 5 0 d から暗号化コンテンツが読み出され、暗号解読鍵で暗号が解読される。

【 0 0 2 4 】

(4) 暗号解読されたコンテンツが圧縮されている場合には、伸張処理（ビデオコンテンツの場合は、M P E G (Motion Picture Experts Group) 伸張処理等）が実行され、得られたコンテンツがRAM 5 0 c 上のバッファに格納された後、MB 5 0 e へ出力される。

【 0 0 2 5 】

(5) MB 5 0 e は、入力されたコンテンツに対してD / A (Digital/Analog) 変換処理および描画処理を施し、得られた音声信号をスピーカ 5 2 (図 7 参照) へ出力するとともに、画像信号を表示装置 5 3 へ出力する。これにより、コンテンツが再生される。

【 0 0 2 6 】

【発明が解決しようとする課題】

ところで、前述したように、従来においては、基本ソフトウェアがパーソナル

コンピュータ 5 0 の R A M 5 0 c に実装されるため、悪意のあるユーザによって解読されたり、コピーされたりするという危険性を伴う。

【 0 0 2 7 】

仮に、ハードディスクドライブ 5 0 d に格納されている基本ソフトウェアやその他を全て暗号化したとしても、その暗号を解くための暗号解読ソフトウェアがパーソナルコンピュータ 5 0 のどこかに存在すれば、その暗号解読ソフトウェアを解析して暗号解読鍵の格納場所が特定されると、やはり基本ソフトウェアが解析され、権利保護アルゴリズムが判明してしまう。

【 0 0 2 8 】

特に、放送等、公共性が高いネットワークでは、権利保護アルゴリズムが判明しても容易にコンテンツの解読ができない処理法が望まれる。現行のハードウェア主体のデジタルテレビ受信機では、M U L T I 2、D E S (Data Encryption Standard) などの暗号化が行われている。これらは、アルゴリズムは公知であるが、暗号解読鍵が判明しない限り、コンテンツの暗号を解読することが極めて困難である。

【 0 0 2 9 】

しかしながら、デジタルテレビ受信機では、暗号解読鍵がハードウェアに内蔵され、ソフトウェア上には読み出すことができないような構成が採られている。

【 0 0 3 0 】

さらに、デジタルテレビ受信機では、暗号解読回路やコンテンツ処理回路 (M P E G ビデオ伸張回路や M P E G オーディオ伸張回路) もハードウェアで構成されているため、処理の内容を覗き見することは極めて困難とされている。

【 0 0 3 1 】

このようなデジタルテレビ受信機は、実際に商用化が進んでいる。日本のパーフェクト TV (商標) や米国の D i r e c T V (商標) などは、かかるデジタルテレビ受信機の好例である。

【 0 0 3 2 】

これに対して、ソフトウェア処理では、暗号解読鍵、暗号解読回路、コンテン

ツ処理回路が基本ソフトウェアで実現されており、このような基本ソフト自体、さらには途中の演算結果も容易に読み取り可能なパーソナルコンピュータ50上のRAM50cに実装されるため、解析、覗き見が容易に行われてしまうという問題があった。

【0033】

本発明は、上記に鑑みてなされたもので、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェアを付加することで、安全なソフトウェア処理を実行することができる情報再生装置および情報再生方法を提供することを目的とする。

【0034】

【課題を解決するための手段】

上記目的を達成するために、本発明は、情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、外部から参照することが可能なメモリと、前記セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスにより前記メモリに格納されたメモリ格納情報を読み出し、該メモリ格納情報と、前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック手段と、を備えたことを特徴とする。

【0035】

また、本発明は、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュール内で実行され、いずれの手段も介さずに直接アクセスにより外部から参照することが可能なメモリに格納されたメモリ格納情報を読み出す読み出し工程と、読み出された前記メモリ格納情報と前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック工程と、を備えたことを特徴とする。

【0036】

この発明によれば、いずれの手段も介さずに直接アクセスによりメモリに格納

されたメモリ格納情報を読み出し、該メモリ格納情報とセキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、メモリ格納情報の改ざんをチェックすることとしたので、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェア（セキュアモジュール）を付加することで、安全なソフトウェア処理を実行することができる。

【 0 0 3 7 】

【発明の実施の形態】

以下、図面を参照して本発明にかかる情報再生装置および情報再生方法の一実施の形態について詳細に説明する。

【 0 0 3 8 】

図 1 は、本発明にかかる一実施の形態の構成を示すブロック図である。同図に示したシステムは、パーソナルコンピュータ 1 0 0、ネットワーク 2 0 0 および表示装置 3 0 0 や、図示しない入力装置、スピーカ等によって構成されており、セキュアな環境で暗号化された情報（コンテンツ）を復号し、再生するためのものである。

【 0 0 3 9 】

パーソナルコンピュータ 1 0 0 は、情報再生装置としての機能を備えており、PCメインプロセッサ 1 0 1、ハードディスクドライブ 1 0 2、入出力インタフェース 1 0 3、サウスブリッジ 1 0 4、ノースブリッジ 1 0 5、メインメモリ 1 0 6、画像 L S I (Large Scale Integrated Circuit) 1 0 7、画像メモリ 1 0 8、P C I (Peripheral Component Interconnect) バス 1 0 9 およびセキュアモジュール 1 5 0 によって構成されている。

【 0 0 4 0 】

また、パーソナルコンピュータ 1 0 0 は、ネットワーク 2 0 0 を介してダウンロードされた暗号化情報（コンテンツ）やハードディスクドライブ 1 0 2 に格納された暗号化情報（コンテンツ）を復号して表示装置 3 0 0 およびスピーカ（図示略）へ出力する。

【 0 0 4 1 】

PCメインプロセッサ101は、ハードディスクドライブ102に格納されているセキュアソフトウェアや、その他のソフトウェアに従って各種演算処理を実行するとともに、装置の各部を制御する。

【0042】

ここで、上記セキュアソフトウェアは、後述する図2～図5に示したセキュアソフトウェア180に対応しており、情報再生に際してセキュアな環境を提供するためのものであり、メインメモリ106に実装される。

【0043】

ハードディスクドライブ102は、ディスクを有する大容量記憶装置であり、PCメインプロセッサ101が実行するセキュアソフトウェア180（図2参照）やその他のソフトウェアを格納している。

【0044】

入出力インタフェース103は、ネットワーク200を介して情報（コンテンツ）を送受信する際のインタフェースであり、プロトコル変換やデータのフォーマット変換を実行する。

【0045】

サウスブリッジ104は、入出力インタフェース103とPCIバス109とを相互接続する機能を備えており、ブリッジ回路を内蔵している。ノースブリッジ105は、PCメインプロセッサ101とメインメモリ106、画像LSI107を相互に接続してデータの橋渡しを行う機能を備えている。なお、サウスブリッジ104とノースブリッジ105とは、高速バスにより相互接続されている。

【0046】

メインメモリ106は、例えば、RAMによって構成されており、図2～図5に示したセキュアソフトウェア180や、その他ソフトウェアが実装されている。セキュアソフトウェア180がPCメインプロセッサ101により実行されることにより、図2～図5に示したセキュアソフトウェア180内の各ブロックの機能が実現される。

【0047】

セキュアソフトウェア180は、メインメモリ106に実装され、PCメインプロセッサ101により実行されることにより、セキュアモジュール150と協調して、セキュアな環境で暗号化されたMP EGデータをデコードする機能等を提供する。

【0048】

画像LSI107は、デコード済みの画像情報を画像メモリ108に格納させたり、表示装置300に画像として表示させる機能を備えている。画像メモリ108は、画像LSI107の制御により、画像情報を格納する。

【0049】

PCIバス109は、ハードディスクドライブ102、サウスブリッジ104および後述するセキュアモジュール150のPCIインタフェース155との間を相互接続するバスである。

【0050】

セキュアモジュール150は、TRM (Tamper Resistant Module) 構造を有しており、外部からの覗き見を防止するとともに、内部のデータが改ざんされることを防止するハードウェアである。

【0051】

TRM構造は、半導体チップ（この場合、セキュアモジュール150）などの内部解析や改ざんを物理的および論理的に防衛するための構造をいう。具体的には、セキュアモジュール150においては、内部に強固で粘着力が高いコーティングが施され、その表面が剥がされると内部の回路が完全に破壊されたり、ダミーの配線が配されている。

【0052】

セキュアモジュール150は、ハードディスクドライブ102からセキュアソフトウェア180（図2～図5参照）等を読み出す機能、メインメモリ106に実装されたセキュアソフトウェア180を不定期に書き換える機能、メインメモリ106に設定された各種バッファの位置を不定期に変更する機能、暗号化機能、復号化機能等を備えている。

【0053】

セキュアモジュール150は、セキュアモジュールプロセッサ151、RAM152、ROM153、暗号復号エンジン154およびPCIインタフェース155、内部バス156から構成されている。セキュアモジュールプロセッサ151は、ROM153に格納されたファームウェアを実行することにより、上述したセキュアモジュール150の各種機能を実現する。

【0054】

RAM152は、セキュアモジュールプロセッサ151が各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。また、RAM152には、暗号鍵等が格納されている。ROM153は、セキュアモジュールプロセッサ151が実行する基本的なファームウェアやデータを格納している。

【0055】

暗号復号エンジン154は、暗号化機能、復号化機能を実現する。PCIインタフェース155は、PCIバス109を介して各部とのインタフェースをとる。内部バス156は、セキュアモジュールプロセッサ151、RAM152、ROM153、暗号復号エンジン154およびPCIインタフェース155の各部を相互接続するバスである。

【0056】

図2～図5には、上述したセキュアソフトウェア180や各種ソフトウェアによって実現される機能（初期化／ロード部160、ドライバ170、入力バッファ181～MPEG出力部188）のブロックが図示されている。これらの図において、図1の各部に対応する部分には同一の符号を付ける。

【0057】

図2に示した初期化／ロード部160は、メインメモリ106（図1参照）に存在し、メインメモリ106上の空き領域を探し、ソフトウェアを当該空きメモリ領域にロード（実装）する機能を備えている。なお、実際には、初期化／ロード部160は、PCメインプロセッサ101でソフトウェアが実行されることにより上記機能を実現する。

【0058】

また、初期化／ロード部 1 6 0 は、パーソナルコンピュータ 1 0 0 の他のアプリケーションソフトウェア（図示略）と連動する必要がある場合、ソフトウェア同士のリンクを設定する機能を備えている。

【 0 0 5 9 】

ここで、パーソナルコンピュータ 1 0 0 において、オペレーティングシステム（図示略）の支配下で他のアプリケーションソフトウェアとセキュアソフトウェア 1 8 0 とがマルチタスク環境で同時に動作する場合には、オペレーティングシステムが各ソフトウェアが動作する時間を割り当てる機能を持つ。

【 0 0 6 0 】

初期化／ロード部 1 6 0 は、セキュアソフトウェア 1 8 0 が実装されたメモリ領域などの情報をオペレーティングシステムへ通知し、セキュアソフトウェア 1 8 0 が動作する時間の割り当てを行うための制御を行う。

【 0 0 6 1 】

これにより、オペレーティングシステムは、例えば、セキュアソフトウェア 1 8 0 が 1 0 0 ミリセカンド動作したら、その後、別のソフトウェアが 1 0 0 ミリセカンド動作するなどのソフトウェア実行に関するスケジューリングを行う。

【 0 0 6 2 】

また、初期化／ロード部 1 6 がオペレーティングシステムと連携を採る理由は、オペレーティングシステムの配下の複数のタスク（プログラム）の一つとしてセキュアソフトウェア 1 8 0 を動かすには、プロセス間の調整を行うオペレーティングシステムの助けが必要だからである。

【 0 0 6 3 】

ドライバ 1 7 0 は、オペレーティングシステムの配下で動作する通常のドライバ用のソフトウェアに対応している。セキュアモジュール 1 5 0 とセキュアソフトウェア 1 8 0 （入力バッファ 1 8 1）との間においては、ドライバ 1 7 0 を経由して、大容量の情報（暗号化 M P E G ストリーム等）が授受される。

【 0 0 6 4 】

つまり、ドライバ 1 7 0 を利用することにより、オペレーティングシステムにおけるドライバ制御用の各種機能が流用可能となる。

【0065】

なお、セキュアモジュール150とセキュアソフトウェア180との間において、上記暗号化MPEGストリーム以外の情報は、DMA(Direct Memory Access)などの直接アクセスにより授受されることが大前提とされる。つまり、セキュアモジュール150とセキュアソフトウェア180とは、ドライバ170を経由せずに直接アクセスすることになる。

【0066】

このように、直接アクセスを大前提とした場合には、オペレーティングシステムがドライバ170へ提供するさまざまなサービスの利用ができなくなるというデメリットが生じる。

【0067】

しかしながら、この場合には、オペレーティングシステムの配下の外となり、オペレーティングシステムが関知しない環境で情報の授受が行えるため、安全性が増大するというセキュリティ上の大きなメリットが生じるのである。

【0068】

例えば、セキュアモジュール150とセキュアソフトウェア180との間でドライバ170を経由して情報が授受された場合には、常に、オペレーティングシステムに対し割り込みが発生し、この割り込みに基づいて、他のソフトウェアが情報を逐次「覗き見」することが可能となり、セキュリティが低くなる。ここで、数あるドライバの中には、情報を他ソフトウェアに転送するという機能がついたドライバも存在する。

【0069】

一方、セキュアモジュール150とセキュアソフトウェア180との間でドライバ170を経由せずに直接アクセスにより情報を授受した場合には、オペレーティングシステムに対し割り込みが発生しない。

【0070】

従って、他のソフトウェアが「覗き見」をする場合には、ポーリングなどにより常にセキュアソフトウェア180の状態（メインメモリ106上のバッファの位置を解析し、バッファ内の情報が更新されたかチェックし、更新された場合に

「覗き見」する）を監視する必要がある。

【 0 0 7 1 】

しかしながら、直接アクセスの場合には、セキュアモジュール 1 5 0 からセキュアソフトウェア 1 8 0 へ情報がいつ到達するかが分からないので、ポーリングするのが実質的に不可能となる。なお、仮にポーリングで一部の情報の「覗き見」ができたとしても、全部のデータの「覗き見」は不可能である。

【 0 0 7 2 】

また、本一実施の形態において、暗号化 M P E G ストリームをドライバ 1 7 0 経由としたのは、M P E G ストリームが暗号化されていて、たとえ盗まれても安全と判断し、ドライバ 1 7 0 の機能を流用し、効率良く暗号化 M P E G ストリームをセキュアソフトウェア 1 8 0 に到達させることを優先させたためである。

【 0 0 7 3 】

入力バッファ 1 8 1 は、メインメモリ 1 0 6 上に領域設定されたバッファであり、暗号化 M P E G ストリームを格納する。T S デコーダ 1 8 2 は、暗号復号部 1 8 4 の要求を受け、バッファ 1 8 1 から暗号化 M P E G ストリーム（正確に言うとは M P E G - T S ストリーム）を読み出し、T S デコード処理した後にビデオバッファ 1 8 3 に暗号化 M P E G ビデオ情報を格納する。

【 0 0 7 4 】

T S デコード処理は、暗号化 M P E G ストリームから、圧縮された暗号化 M P E G ビデオ情報を抽出する処理である。暗号化 M P E G ストリームには、時分割多重された形で（１）暗号化 M P E G ビデオ情報、（２）暗号化 M P E G オーディオ情報、（３）暗号化 M P E G ビデオ情報と暗号化 M P E G オーディオ情報により構成される番組情報（番組の名称、放送時期、番組のあらすじ、番組の料金など）が含まれている。

【 0 0 7 5 】

なお、実際のセキュアソフトウェアでは、暗号化 M P E G ビデオ情報に加えて、暗号化 M P E G オーディオ情報もデコードする必要がある。その場合の暗号化 M P E G オーディオ情報のデコードについては、暗号化 M P E G ビデオ情報のデコードと同種のプログラムが必要になることは言うまでもない。

【 0 0 7 6 】

また、T S デコーダ 1 8 2 は、入力バッファ 1 8 1 の容量を常に監視し、それが一定水準以下になると、セキュアソフトウェア 1 8 0 へ入力バッファ 1 8 1 の補給を依頼する。

【 0 0 7 7 】

ビデオバッファ 1 8 3 は、メインメモリ 1 0 6 上に領域設定されたバッファであり、上述した暗号化 M P E G ビデオ情報を格納する。このビデオバッファ 1 8 3 は、M P E G ビデオの国際規格で定められた V B V バッファに相当するバッファである。

【 0 0 7 8 】

暗号復号部 1 8 4 は、M P E G ビデオデコーダ 1 8 6 の要求を受け、ビデオバッファ 1 8 3 から暗号化 M P E G ビデオ情報を読み出し、小バッファ 1 8 5 が一杯になるまで暗号化 M P E G ビデオ情報を復号する。また、暗号復号部 1 8 4 は、復号済みの圧縮 M P E G ビデオ情報を小バッファ 1 8 5 へ格納する。

【 0 0 7 9 】

小バッファ 1 8 5 は、メインメモリ 1 0 6 上に領域設定されたバッファであり、上述した圧縮 M P E G ビデオ情報を格納する。M P E G ビデオデコーダ 1 8 6 は、後段の M P E G 出力部 1 8 8 が画像情報を出力したことを認識する。

【 0 0 8 0 】

ここで、M P E G 画像メモリ 1 8 7 に出力した画像情報分の空き領域ができるため、M P E G ビデオデコーダ 1 8 6 は、小バッファ 1 8 5 から次の 1 枚分の圧縮 M P E G ビデオ情報を読み出し、伸張処理（デコード）を行った後、画像情報を M P E G 画像メモリ 1 8 7 に格納する。

【 0 0 8 1 】

また、小バッファ 1 8 5 は、少量（画像 1 枚未満）の圧縮 M P E G ビデオ情報しか格納できないように設定されている。これは、復号済みの圧縮 M P E G ビデオ情報をメインメモリ 1 0 6 上に存在させることがセキュリティ上非常に危険であり、この危険を回避するためのである。

【 0 0 8 2 】

従って、小バッファ 1 8 5 は、画像 1 枚分の圧縮 M P E G ビデオ情報を保持することはなく、M P E G ビデオデコーダ 1 8 6 でデコードが開始されてから間もなく「空」になる。

【 0 0 8 3 】

また、M P E G ビデオデコーダ 1 8 6 は、小バッファ 1 8 5 が「空」になるか、または小バッファ 1 8 5 内の情報量が、予め設定されたしきい値より小さくなった時点で、暗号復号部 1 8 4 に対して復号要求を出し、小バッファ 1 8 5 に圧縮 M P E G ビデオ情報を格納させる。

【 0 0 8 4 】

M P E G 画像メモリ 1 8 7 は、例えば、4 フレーム分、即ち 3 0 分の 4 秒分（約 1 3 3 ミリセカンド）に対応する画像情報を格納する。M P E G 出力部 1 8 8 は、M P E G 画像メモリ 1 8 7 から伸張（デコード）済みの画像情報（1 枚分または 1 フレーム分）を読み出し、これを画像 L S I 1 0 7 へ DMA 転送する。ここで、DMA（直接アクセス）を使うのは、M P E G 出力部 1 8 8 から画像 L S I 1 0 7 への転送を高速に行うためである。

【 0 0 8 5 】

一実施の形態では、メインメモリ 1 0 6 に設定されたビデオバッファ 1 8 3 に暗号化された暗号化 M P E G ビデオ情報を格納する点と、ビデオバッファ 1 8 3 に格納された暗号化 M P E G ビデオ情報を少しずつ復号化し、小バッファ 1 8 5 に格納しながら M P E G ビデオデコードを実行する点に特徴がある。

【 0 0 8 6 】

図 3 に示したセキュアモジュール 1 5 0 において、メモリ空間 1 5 2 A は、R A M 1 5 2（図 1 参照）に設定されており、セキュアモジュール 1 5 0 と T S デコーダ 1 8 2 との間で実行される第 1 の秘密番号通信で用いられる。

【 0 0 8 7 】

セキュアモジュール 1 5 0（セキュアモジュールプロセッサ 1 5 1）は、メモリ空間 1 5 2 A について 1 度目は正規の値、2 度目は違う値が読み出されるように、制御する。

【 0 0 8 8 】

メモリ空間 1 5 2 B は、RAM 1 5 2（図 1 参照）に設定されており、セキュアモジュール 1 5 0 と暗号復号部 1 8 4 との間で実行される第 2 の秘密番号通信で用いられる。

【 0 0 8 9 】

セキュアモジュール 1 5 0（セキュアモジュールプロセッサ 1 5 1）は、メモリ空間 1 5 2 A と同様にして、メモリ空間 1 5 2 B について 1 度目は正規の値、2 度目は違う値が読み出されるように、制御する。

【 0 0 9 0 】

（電源投入時のセキュア機能）

つぎに、図 2 を参照して、図 1 に示したパーソナルコンピュータ 1 0 0 における電源投入時のセキュア機能について説明する。

【 0 0 9 1 】

図 2 には、パーソナルコンピュータ 1 0 0 の電源投入時に、初期化／ロード部 1 6 0 がセキュアモジュール 1 5 0 からセキュアソフトウェア 1 8 0 をメインメモリ 1 0 6 にロードする場合について図示されている。

【 0 0 9 2 】

同図において、パーソナルコンピュータ 1 0 0 に電源が投入されると、オペレーティングシステムが起動され、デスクトップ（図示略）に起動すべきソフトウェア（プログラム、アプリケーション）のリストが表示される。

【 0 0 9 3 】

これにより、ユーザは、上記リストを見て所望のソフトウェアとして、例えば、セキュアソフトウェア 1 8 0 を起動させる。具体的には、ユーザにより、デスクトップに表示されたセキュアソフトウェア 1 8 0 に対応するアイコンがクリックされると、セキュアソフトウェア 1 8 0 が起動される。

【 0 0 9 4 】

つまり、初期化／ロード部 1 6 0 は、セキュアモジュール 1 5 0 に対して、セキュアソフトウェア 1 8 0 のロードを要求する。なお、一般の初期化／ロード部は、ハードディスクドライブ 1 0 2 からソフトウェアを直接ロードするが、一実施の形態では、セキュアモジュール 1 5 0 を経由している。

【 0 0 9 5 】

セキュアモジュール 1 5 0（セキュアモジュールプロセッサ 1 5 1）は、ハードディスクドライブ 1 0 2 からセキュアソフトウェア 1 8 0 を読み出した後、このセキュアソフトウェア 1 8 0 の特定部分（例えば、秘密の番号が記述された部分）を変更する。つぎに、セキュアモジュール 1 5 0 は、変更後のセキュアソフトウェア 1 8 0 を初期化／ロード部 1 6 0 へ渡す。

【 0 0 9 6 】

初期化／ロード部 1 6 0 は、メインメモリ 1 0 6 上の空き領域を探し、当該空き領域に変更後のセキュアソフトウェア 1 8 0 をロード（実装）する。

【 0 0 9 7 】

ここで、パーソナルコンピュータ 1 0 0 上のメモリ空間は、セキュアモジュール 1 5 0 から DMA など直接アクセスできることが前提とされており、例えば、メインメモリ 1 0 6 上のスワップ不可能領域である必要がある。スワップ不可能領域の獲得は、オペレーティングシステムの機能を利用すればよい。

【 0 0 9 8 】

仮に、スワップ可能領域にセキュアソフトウェア 1 8 0 が実装された場合、セキュアソフトウェア 1 8 0 は、メインメモリ 1 0 6 上からハードディスクドライブ 1 0 2 のメモリ空間などにオペレーティングシステムの機能で自動的にスワップされる可能性がある。

【 0 0 9 9 】

スワップされるのは、同時に複数のソフトウェアが動作し、パーソナルコンピュータ 1 0 0 上のメインメモリ 1 0 6 に全部のソフトウェアが搭載出来なくなるためである。

【 0 1 0 0 】

しかしながら、かかる場合には、セキュアソフトウェア 1 8 0 がメインメモリ 1 0 6 上に存在しない可能性があり、セキュアモジュール 1 5 0 から DMA など直接アクセスできなくなるという問題が発生する。

【 0 1 0 1 】

そこで、一実施の形態では、ロード時にセキュアモジュール 1 5 0 をスワップ

不可能領域に実装し、セキュアモジュール 1 5 0 から常にセキュアソフトウェア 1 8 0 の実装位置が分かるようにしている。以上が、電源投入から、セキュアソフトウェア 1 8 0 がメインメモリ 1 0 6 にロードされるまでの動作例である。

【 0 1 0 2 】

また、上述のように、電源投入時に初期化／ロード部 1 6 0 を介した場合には、オペレーティングシステムとリンクを貼ることができるので（１）プログラムのバッファ領域、（２）全体のプログラムコード、（３）プログラムの存在するメモリ領域などを全面的に変更することが可能となる。

【 0 1 0 3 】

（通常動作時のセキュア機能）

つぎに、図 3 を参照して、図 1 に示したパーソナルコンピュータ 1 0 0 における電源投入後の通常動作時のセキュア機能について説明する。

【 0 1 0 4 】

図 3 においては、パーソナルコンピュータ 1 0 0 のメインメモリ 1 0 6 にセキュアソフトウェア 1 8 0 がロード（実装）されている。

【 0 1 0 5 】

この場合、セキュアソフトウェア 1 8 0 は、例えば以下のような動作を行う。同図においては、最終的に画像情報を消費しているのが表示装置 3 0 0 であり、画像 L S I 1 0 7 と連動していると考ええる。

【 0 1 0 6 】

まず、画像 L S I 1 0 7 が表示装置 3 0 0 にある画像を表示し終わると、次の画像を表示するための準備をセキュアソフトウェア 1 8 0 に依頼する。これにより、M P E G 出力部 1 8 8 は、M P E G 画像メモリ 1 8 7 から画像情報（１枚分）を読み出し、これを画像 L S I 1 0 7 へ DMA 転送する。

【 0 1 0 7 】

暗号復号部 1 8 4 は、M P E G ビデオデコーダ 1 8 6 の要求を受け、ビデオバッファ 1 8 3 から暗号化 M P E G ビデオ情報を取り出し、小バッファ 1 8 5 が一杯になるまで暗号化 M P E G ビデオ情報を復号する。復号時、暗号復号部 1 8 4 は、セキュアモジュール 1 5 0 から復号鍵を授受する。

【0108】

復号鍵は、ある限られた時間（例えば数秒間）しか有効でなく、それ以降は、新規に復号鍵をセキュアモジュール150から授受する必要がある。セキュアモジュール150から復号鍵を授受するアルゴリズムは、例えば、後述する第2の秘密番号通信に含まれてもよい。

【0109】

これにより、セキュアモジュール150は、セキュアソフトウェア180が秘密の番号を知っていることを確認しつつ、復号鍵を安心してセキュアソフトウェア180へ提供することが可能となる。

【0110】

また、暗号復号部184は、ビデオバッファ183の暗号化MPEGビデオ情報の残存量を常に監視しており、これが一定量以下になったら、TSデコーダ182に暗号化MPEGビデオ情報の補給を依頼する。

【0111】

つぎに、TSデコーダ182は、暗号復号部184からの上記依頼を受け、入力バッファ181から暗号化MPEGストリームを読み出し、TSデコード処理を施す。つぎに、TSデコーダ182は、暗号化MPEGビデオ情報をビデオバッファ183へ格納する。

【0112】

また、TSデコーダ182は、入力バッファ181の容量を常に監視し、それが一定水準以下になると、セキュアモジュール150へ暗号化MPEGストリームの補給を依頼する。

【0113】

これにより、セキュアモジュール150は、ハードディスクドライブ102より暗号化された暗号化MPEGストリームを読み出す。つぎに、セキュアモジュール150の暗号復号エンジン154は、一旦、暗号化MPEGストリームを復号した後、別の暗号鍵で再暗号化する。この再暗号化された暗号化MPEGストリームがセキュアモジュール150からセキュアソフトウェア180へ提供される。

【0114】

ここで、再暗号化するのは、ハードディスクドライブ102から読み出された暗号化MPEGストリームをそのままセキュアソフトウェア180へ提供した場合、パーソナルコンピュータ100で最もセキュリティーが低いセキュアソフトウェア180に復号鍵を渡すことになり、危険だからである。

【0115】

これに対して、セキュアモジュール150において再暗号化した場合には、ハードディスクドライブ102に格納された暗号化MPEGストリームではなく、そのときのセキュアソフトウェア180用に再暗号化した、そのときのセキュアソフトウェア180でしか使えない暗号化MPEGストリームがセキュアソフトウェア180へ提供される。

【0116】

従って、いついかなるときでも読み出せるハードディスクドライブ102内の暗号化MPEGストリームよりも、再暗号化した暗号化MPEGストリームのほうが危険が少ない。

【0117】

また、図3においては、上述した動作に並行して、セキュアソフトウェア180の安全性を確認するための動作が実行される。この動作においては、次の(1)～(4)に示した処理が実行され、セキュアモジュール150がセキュアソフトウェア180に様々な作用を及ぼし、応答等が授受される。

【0118】

- (1) スキャン認証処理
- (2) プログラムを不定期に書き換える処理
- (3) バッファの位置を不定期に書き換える処理
- (4) 秘密の番号通信処理

【0119】

ここで、(1)～(4)において、(1)～(3)は、セキュアモジュール150により実行される。(4)は、セキュアモジュール150およびセキュアソフトウェア180により実行される。

【 0 1 2 0 】

以下では、（１）～（４）の処理について順次説明する。はじめに、（１）スキャン認証処理について説明する。

【 0 1 2 1 】

スキャン認証処理において、セキュアモジュール 1 5 0 は、動作中のセキュアソフトウェア 1 8 0 が実装されているメインメモリ 1 0 6 の一部領域または全領域に DMA など直接アクセスし、セキュアソフトウェア 1 8 0 のデータの一部または全部を読み出す。

【 0 1 2 2 】

つぎに、セキュアモジュール 1 5 0 は、読み出したデータと、RAM 1 5 2 （図 1 参照）等に予め格納されたデータとを比較し、一致するか否かにより認証を行う。例えば、悪意のあるユーザによりセキュアソフトウェア 1 8 0 が改ざんされている場合には、プログラムが書き換えられているため、上記比較結果が不一致とされ、認証 NG とされる。

【 0 1 2 3 】

一方、セキュアソフトウェア 1 8 0 が改ざんされていない場合には、上記比較結果が一致とされ、認証 OK とされる。

【 0 1 2 4 】

具体的な実現方法としては、セキュアモジュール 1 5 0 の RAM 1 5 2 に、セキュアソフトウェア 1 8 0 と同内容を格納し、メインメモリ 1 0 6 からセキュアソフトウェア 1 8 0 を DMA など直接に読み出し、その結果と RAM 1 5 2 に格納されている内容と逐一比較する方法がある。

【 0 1 2 5 】

また、一実施の形態では、セキュアモジュール 1 5 0 の RAM 1 5 2 のメモリ容量が小さくセキュアソフトウェア 1 8 0 の全てを格納できない場合には、チェックサムのような方法によりスキャン認証処理を行ってもよい。

【 0 1 2 6 】

すなわち、この場合には、セキュアソフトウェア 1 8 0 のコードを全部加算した結果だけを RAM 1 5 2 に格納しておき、メインメモリ 1 0 6 からセキュアソ

フトウェア 1 8 0 を DMA で読み出した後、コードを加算した結果と RAM 1 5 2 に格納された内容とを比較し、比較結果が一致した場合は、セキュアソフトウェア 1 8 0 が改ざんされていないと判断される（認証結果＝OK）。

【 0 1 2 7 】

また、スキャン認証による改ざんの検出は、セキュアモジュール 1 5 0 がセキュアソフトウェア 1 8 0 と関係なく単独でセキュアソフトウェア 1 8 0 が実装されているメインメモリ 1 0 6 に直接アクセスすることにより行われる。

【 0 1 2 8 】

また、スキャン認証処理は、オペレーティングシステムを一切経由しないのでオペレーティングシステムの機能などを流用した改ざんや覗き見に対しても安全性が強い。

【 0 1 2 9 】

これに対して、オペレーティングシステムを経由した場合には、例えば、「いつスキャン認証処理が実行されているか」をオペレーティングシステムへ通知される割り込み情報などで悪意のユーザに簡単に知られてしまう可能性が高いのである。

【 0 1 3 0 】

次に、（２）プログラムを不定期に書き換える処理について説明する。プログラムを不定期に書き換える処理において、セキュアモジュール 1 5 0 （セキュアモジュールプロセッサ 1 5 1）は、セキュアソフトウェア 1 8 0 が動作中に、セキュアソフトウェア 1 8 0 が実装されたメモリ領域（メインメモリ 1 0 6）に対して、直接に DMA 転送などで書き込みをリアルタイムで行う。

【 0 1 3 1 】

ここで、前述した（１）スキャン認証処理が読み出し動作であるのに対して、（２）プログラムを不定期に書き換える処理では、書き込み動作を行う。具体的には、オペレーティングシステムにわからないように、セキュアモジュール 1 5 0 がオペレーティングシステムを介さずセキュアソフトウェア 1 8 0 のプログラムなどの一部を書き換える。

【 0 1 3 2 】

これにより、後にスキャン認証処理を実行した場合に、セキュアソフトウェア 180 が動作している最中でも、認証結果がリアルタイムで変化し、スキャン認証処理における安全度が向上する。

【0133】

ここで、スキャン認証とプログラムの不定期の書き換えとの相乗効果について説明する。図2においては、例えば、セキュアソフトウェア180の中の「秘密の番号通信を行うためのプログラム」を書き換える。

【0134】

この場合には、リアルタイムで書き換え、その後、その書き換えたプログラムのコードに対し、スキャン認証処理を実行するため安全度が向上する。悪意のあるユーザ（ハッカー）が如何に有能であっても、リアルタイムに変化するプログラムをハッキングすることが困難であることは、容易に想像される。

【0135】

また、一実施の形態では、書き換えたプログラムの実動作を確認することで、本当に実動作中のプログラムが書き換わっていることを確認することもできる。これは、以下の攻撃に対して有効である。

【0136】

すなわち、悪意のあるユーザは、スキャン認証を誤魔化するため、スキャン認証用（誤魔化し用）の「セキュアソフトウェアa」と、実際に動作する「セキュアソフトウェアb」というのセキュアソフトウェアをパーソナルコンピュータ100のメインメモリ106に並列的に実装し、「セキュアソフトウェアa」を対象としてスキャン認証処理を実行させ、実動作は「セキュアソフトウェアb」が行うような攻撃が考えられる。

【0137】

スキャン認証の目的は、プログラムの書き換えを不可能にすることである。しかしながら、偽の「セキュアソフトウェアa」を作ること、悪意のあるユーザによって、「セキュアソフトウェアb」を自由に書き換えられ、スキャン認証が誤魔化される。

【0138】

また、初期化／ロード部160がセキュアソフトウェア180をロードする場合には、セキュアモジュール150に対してロード先のメモリ領域を通知している。

【0139】

しかしながら、その時、初期化／ロード部160がセキュアモジュール150に偽のメモリ領域としてセキュアソフトウェアaのメモリ領域を通知することにより、上述した攻撃が可能となる。

【0140】

これに対して、一実施の形態では、リアルタイムでセキュアソフトウェア180の一部（または全部）を書き換え、その書き換えた結果で、セキュアソフトウェア180の実動作を変化させ、その変化をセキュアモジュール150が検知することでセキュアソフトウェア180の安全性をさらに向上させることができる。

【0141】

一実施の形態において変更されるのは、例えば、「秘密の番号通信プログラム」である。この「秘密の番号通信プログラム」は、セキュアソフトウェア180の中に、セキュアモジュール150とセキュアソフトウェア180との間で「秘密の番号」を通信し、セキュアモジュール150がセキュアソフトウェア180の安全性を確認するためのプログラムである。

【0142】

例えば、セキュアモジュール150から秘密の番号をセキュアソフトウェア180へ通知した後、セキュアソフトウェア180がセキュアモジュール150へ正規の秘密の番号を返信する。

【0143】

ここで、正規の秘密の番号以外の番号がセキュアモジュール150へ返信された場合、セキュアモジュール150は、セキュアソフトウェア180が改ざんされたと判断する。秘密の番号は、複数の番号からなる番号シーケンスであっても良い。

【0144】

このように、一実施の形態では、セキュアモジュール 1 5 0 が、DMA などの方法で直接にセキュアソフトウェア 1 8 0 に対してスキャン認証処理を実行し、コードの一部をリアルタイムで書き換え、そのコードが動作していることを確認することにより、上述した攻撃を防ぐことができる。

【 0 1 4 5 】

以上では、「成り済まし」プログラムを検出する構成例について説明した。「成り済まし」を発見したら、セキュアモジュール 1 5 0 は、セキュアソフトウェア 1 8 0 の暗号復号部 1 8 4 への復号鍵の提供を中止する。

【 0 1 4 6 】

セキュアモジュール 1 5 0 では、複数の復号鍵が存在し、各復号鍵が、例えば、数秒間しか有効でない。従って、復号鍵の提供が停止されると、数秒後には、セキュアソフトウェア 1 8 0 で、暗号化 M P E G ストリームにかかる一連の処理を続行できなくなる。

【 0 1 4 7 】

つぎに、(3) バッファの位置を不定期に書き換える処理について説明する。(3) の処理では、前述した (1) および (2) の処理によりセキュアソフトウェア 1 8 0 の安全性を確認しつつ、さらにセキュアソフトウェア 1 8 0 が使うバッファ (データ領域) をリアルタイムで変更することで「覗き見」攻撃に対処する。

【 0 1 4 8 】

ここで、「覗き見」とは、セキュアソフトウェア 1 8 0 の中のデータ領域を本プログラムと同時に (時分割に) 動作する他のプログラムが「覗き見」し、情報を盗むことである。

【 0 1 4 9 】

本来、パーソナルコンピュータ 1 0 0 におけるメモリ空間は、時分割に動作するどのプログラムからも「覗き見」が可能である。これは、現状のプロセッサがどのメモリ領域もアクセスできるように設計されていて、プログラムごとにメモリ空間のアクセスを制御する機構がないためである。

【 0 1 5 0 】

最近では、オペレーティングシステムレベルでプログラムごとにアクセスできるメモリ空間を制御できるものも散見されるが、決して十分でない。悪意のあるユーザがその気になれば、簡単に他のメモリ空間の「覗き見」が可能であり、セキュアソフトウェア180の構造を解析し、どこに肝心なデータがあるかを見つけ出して「覗き見」によりデータを盗むことが可能である。

【0151】

例えば、図3に示したセキュアソフトウェア180では、入力バッファ181、ビデオバッファ183、小バッファ185、MPEG画像メモリ187（総称してバッファという）の位置が特定されれば、そのメモリ空間を「覗き見」することで、MPEGストリーム情報などを盗むことが可能である。

【0152】

特に、復号済みの生の圧縮MPEGビデオ情報が格納された小バッファ185は、扱い易く、悪意のあるユーザの攻撃の標的になり易い。MPEG画像メモリ187は、例え位置が特定されても、デコード済みの大容量の画像情報が格納されている。

【0153】

従って、上記画像情報をハードディスクドライブ102に蓄積し盗むことは、ハードディスクドライブ102のデータ転送スピード、ハードディスクドライブ102に繋がるPCIバス109などの転送スピードを考慮すると困難である。

【0154】

そこで、一実施の形態では、バッファの位置を不定期に書き換える、すなわち、バッファの開始番地などをDMAでプログラムコードを書き換えることにより、「覗き見」による情報の盗難を困難にしている。

【0155】

つぎに、（4）秘密の番号通信処理について説明する。秘密の番号通信処理では、図3に示したセキュアモジュール150は、セキュアソフトウェア180のある領域にデータ（最初の秘密番号など）を書き込む（第1および第2の秘密番号通信）。

【0156】

つぎに、このデータをセキュアソフトウェア180が確認し、適当な番号を返すことで、セキュアモジュール150は、セキュアソフトウェア180の安全性を確認する。

【0157】

秘密の番号は、単独の番号の他に、シーケンス番号であったり、テキスト情報であってもよい。当然ながら、この秘密の番号は、セキュアモジュール150とセキュアソフトウェア180しか知らない情報である。従って、先ほどの「覗き見」解析などでこの番号が解析されないため、秘密の番号は、毎回、セキュアモジュール150により変更される。

【0158】

また、秘密の番号通信処理においては、セキュアモジュール150からセキュアソフトウェア180のメモリ領域にデータが書き込まれた場合には、それを「覗き見」される危険がある。

【0159】

そこで、一実施の形態では、上記危険を回避するために、セキュアモジュール150内に1度読み出すと正規の値が読めるが、2度目は違う値（例えば、「0」）が読み出されるメモリ空間152Aおよび152Bを設けて、これらのメモリ空間152Aおよび152Bを介してデータのやり取りが行われる。

【0160】

また、一実施の形態では、1度読み出すと正規の値で2度目は「0」が出るメモリ空間152B等を利用して、セキュアモジュール150とセキュアソフトウェア180との間で復号鍵や暗号鍵などの情報が授受される。なお、メモリ空間152Aおよび152Bは、当然のことながら、暗号鍵以外の情報の伝達にも使用可能である。

【0161】

（全切替時のセキュア機能）

つぎに、図4を参照して、図1に示したパーソナルコンピュータ100における全切替時のセキュア機能について説明する。

【0162】

図4には、パーソナルコンピュータ100のメインメモリ106にロード（実装）されたセキュアソフトウェア180の通常動作中に初期化／ロード部160を用いて、セキュアソフトウェア180の全てを別のセキュアソフトウェア180'（TSデコーダ182'、暗号復号部184'、MPEGビデオデコーダ186'、MPEG出力部188'等）に切り替える場合が図示されている。

【0163】

全切替時において、メインメモリ106上には、変更前のセキュアソフトウェア180と変更後のセキュアソフトウェア180'とが、一時期、並列的に存在する。

【0164】

これは、動作中にセキュアソフトウェア180を停止させると、例えば、MPEGの画像再生が途中で停止したりする可能性があり、これを避けるための処置である。

【0165】

ここで、セキュアソフトウェア180をメインメモリ106から削除した後に、セキュアソフトウェア180'を初期化／ロード部160よりロードした場合には、時間がかかり、MPEGの画像再生が停止するという事態が発生する。

【0166】

一実施の形態では、上記事態を回避するために、初期化／ロード部160により、セキュアソフトウェア180を削除する前に、セキュアソフトウェア180'を予めメインメモリ106にロードする。これにより、セキュアソフトウェア180からセキュアソフトウェア180'への移行時間が短縮される。

【0167】

また、セキュアソフトウェア180からセキュアソフトウェア180'へ切替を行う場合には、セキュアソフトウェア180が使っていたバッファ領域の引継ぎも必要である。

【0168】

例えば、図2および図3においては、ビデオバッファ183に数秒分の暗号化MPEGビデオ情報が格納されている可能性があり、MPEG画像メモリ187

に例えば4フレーム分、即ち30分の4秒分（約133ミリセカンド）の画像情報が格納されている可能性がある。

【0169】

しかも、ビデオバッファ183に何秒分の暗号化MPEGビデオ情報が格納されているかは、MPEGビデオのデコード処理を実行しないと分からない。

【0170】

これは、MPEGの圧縮率が画像に依存し、圧縮容易な画像の場合、たくさんの画像を蓄積できるが、圧縮効率の悪い画像（動画成分が多く、いちいち更新しなくてはならない画像）の場合は、少ししかビデオバッファ183に格納できないためである。このため、一実施の形態では、処理途中のバッファ情報をセキュアソフトウェア180'がセキュアソフトウェア180から引き継ぐ必要がある。

【0171】

通常、セキュアソフトウェアを初期化／ロード部160を使用し切り替える（変更する）のは、以下の理由による。セキュアソフトウェアは、セキュアモジュール150による直接の書き込み（DMA）でリアルタイムに変更されている。

【0172】

しかしながら、この変更では、セキュアソフトウェアの一部を変更するだけで、セキュアソフトウェア全体を変更するのが困難である。セキュアソフトウェアを全体的に変更するには、やはり初期化／ロード部160を経由し、抜本的にやる必要がある。このため、一実施の形態では、初期化／ロード部160による変更も可能な構成としている。

【0173】

具体的には、セキュアモジュール150は、初期化／ロード部160に対して、セキュアソフトウェアの切替要求を出す。これにより、初期化／ロード部160は、セキュアモジュール150へロード要求を出す。セキュアモジュール150は、初期化／ロード部160の要求に応じて、前述した動作と同様にして、「変更されたセキュアソフトウェア180'」を初期化／ロード部160へ渡す。

【0174】

ここで、セキュアモジュール 1 5 0 が、最初の切替え要求を初期化／ロード部 1 6 0 へ出す理由は、セキュアモジュール 1 5 0 から出した方が、オペレーティングシステムに近い初期化／ロード部 1 6 0 から出すより安全であり、オペレーティングシステムから何時セキュアソフトウェアの切り替えが行われたかをわからなくするためである。

【 0 1 7 5 】

次に、初期化／ロード部 1 6 0 は、パーソナルコンピュータ 1 0 0 上のスワップ不可能空きメモリ領域を見つけてメインメモリ 1 0 6 にセキュアソフトウェア 1 8 0' をロードする。

【 0 1 7 6 】

そして、セキュアモジュール 1 5 0 は、切替の制御を行う。例えば、セキュアモジュール 1 5 0 は、セキュアソフトウェア内のあるメモリ空間に特別の番号を書き込むことで切替の制御を行う。

【 0 1 7 7 】

次に、セキュアソフトウェア 1 8 0 からセキュアソフトウェア 1 8 0' へ制御が移行される。但し、制御を移行する際には、セキュアソフトウェア 1 8 0 が使っていたバッファメモリ空間の制御をセキュアソフトウェア 1 8 0' へ移行させる必要がある。

【 0 1 7 8 】

このため、以下のような具体的な制御が実行される。

【 0 1 7 9 】

(1) セキュアモジュール 1 5 0 が切り替え要求信号を初期化／ロード部 1 6 0 に渡す。

【 0 1 8 0 】

(2) 初期化／ロード部 1 6 0 がセキュアモジュール 1 5 0 にセキュアソフトウェア 1 8 0' を要求する。

【 0 1 8 1 】

(3) セキュアモジュール 1 5 0 は、セキュアソフトウェア 1 8 0' を初期化／ロード部 1 6 0 へ渡す。

【 0 1 8 2 】

(4) 初期化／ロード部 1 6 0 は、セキュアソフトウェア 1 8 0' をメインメモリ 1 0 6 上のスワップ不可能領域にロードする。

【 0 1 8 3 】

(5) これで、セキュアソフトウェア 1 8 0 とセキュアソフトウェア 1 8 0' とがメインメモリ 1 0 6 上に並列的に存在することになる。

【 0 1 8 4 】

(6) セキュアモジュール 1 5 0 がセキュアソフトウェア 1 8 0 へセキュアソフトウェア切替指示を出す。

【 0 1 8 5 】

(7) セキュアソフトウェア切替指示を受けたセキュアソフトウェア 1 8 0 は、MPEG 処理の切りのいい所で制御を、セキュアソフトウェア 1 8 0' に移行させるため、画像 L S I 1 0 7 からの画像表示終了信号の入力を待ち、画像表示終了信号が入力されたところで、以下の処置を講ずる。

【 0 1 8 6 】

(a) セキュアソフトウェア 1 8 0 は、MPEG 画像メモリ 1 8 7 の開始番地と関連情報をセキュアソフトウェア 1 8 0' へ通知する。関連情報は、例えば、MPEG 画像メモリ 1 8 7 が 4 フレーム構造の場合、各 MPEG フレームの種類（I ピクチャ、P ピクチャ、B ピクチャ）や、更新可能なフレーム、次のフレームに表示すべき画像等に関する情報である。

【 0 1 8 7 】

(b) セキュアソフトウェア 1 8 0 は、小バッファ 1 8 5 のメモリ開始番地とデータ残存量に関する情報をセキュアソフトウェア 1 8 0' へ通知する。

【 0 1 8 8 】

(c) セキュアソフトウェア 1 8 0 は、ビデオバッファ 1 8 3 のメモリ開始番地とデータ残存量に関する情報をセキュアソフトウェア 1 8 0' へ通知する。

【 0 1 8 9 】

(d) セキュアソフトウェア 1 8 0 は、入力バッファ 1 8 1 のメモリ開始番地とメモリ残存量に関する情報をセキュアソフトウェア 1 8 0' に通知する。

【0190】

(e) セキュアソフトウェア180は、使用中の暗号鍵や復号鍵の情報をセキュアソフトウェア180'へ通知する。

(8) セキュアソフトウェア180は、セキュアソフトウェア180'に制御を移行させる。

【0191】

(一部切替時のセキュア機能)

つぎに、図5を参照して、図1に示したパーソナルコンピュータ100における一部切替時のセキュア機能について説明する。

【0192】

図5には、パーソナルコンピュータ100のメインメモリ106にロード（実装）されたセキュアソフトウェア180の通常動作中に初期化／ロード部160を用いて、セキュアソフトウェア180の一部（例えば、MPEGビデオデコーダ186）を、別のMPEGビデオデコーダ186'に切り替える場合が図示されている。

【0193】

ここで、前述した図4においては、セキュアソフトウェア180の全部をセキュアソフトウェア180'に切り替える場合について説明したが、一部を切り替える図5の場合が实际的である。図5の場合には、セキュアソフトウェア180の一部しか切り換えられないため、バッファも一部しか、引き継がない。

【0194】

全切替時の(1)～(5)の動作を経て、以下の動作が行われる。

【0195】

(6') セキュアモジュール150がセキュアソフトウェア180へセキュアソフトウェア切替指示を出す。

【0196】

(7') セキュアソフトウェア切替指示を受けたセキュアソフトウェア180は、MPEG処理の切りのいい所で制御を、MPEGビデオデコーダ186をMPEGビデオデコーダ186'に移行させるため、画像LSI107からの画像表

示終了信号の入力を待ち、画像表示終了信号が入力されたところで、以下の処置を講ずる。

【 0 1 9 7 】

(a ') セキュアソフトウェア 1 8 0 は、M P E G 画像メモリ 1 8 7 の開始番地と関連情報をM P E G ビデオデコーダ 1 8 6 ' へ通知する。関連情報は、例えば、M P E G 画像メモリ 1 8 7 が4 フレーム構造の場合、各M P E G フレームの種類 (I ピクチャ、P ピクチャ、B ピクチャ) や、更新可能なフレーム、次のフレームに表示すべき画像等に関する情報である。

【 0 1 9 8 】

(b ') セキュアソフトウェア 1 8 0 は、小バッファ 1 8 5 のメモリ開始番地とデータ残存量に関する情報をM P E G ビデオデコーダ 1 8 6 ' へ通知する。

【 0 1 9 9 】

(8 ') セキュアソフトウェア 1 8 0 は、M P E G ビデオデコーダ 1 8 6 に換えて、M P E G ビデオデコーダ 1 8 6 ' を正式のM P E G ビデオデコーダとして組み込み、処理を開始する。

【 0 2 0 0 】

なお、ビデオバッファ 1 8 3 や、入力バッファ 1 8 1 は、M P E G ビデオデコーダ 1 8 6 と直接の関連がないため切り替える必要はない。

【 0 2 0 1 】

以上説明したように、一実施の形態によれば、図 3 に示したセキュアモジュール 1 5 0 を設け、セキュアモジュール 1 5 0 からセキュアソフトウェア 1 8 0 が格納されたメインメモリ 1 0 6 へ直接アクセスすることにより、プログラムの書き換え、バッファ位置の変更、スキャン認証等を実行するようにしたので、パーソナルコンピュータ 1 0 0 等のオープンアーキテクチャを有する装置に対して、最低限のハードウェア (セキュアモジュール 1 5 0) を付加することで、安全なソフトウェア処理を実行することができる。

【 0 2 0 2 】

以上本発明にかかる一実施の形態について図面を参照して詳述してきたが、具体的な構成例はこの一実施の形態に限られるものではなく、本発明の要旨を逸脱

しない範囲の設計変更等があっても本発明に含まれる。

【0203】

例えば、前述した一実施の形態においては、前述したセキュア機能を実現するためのプログラムを図6に示したコンピュータ読み取り可能な記録媒体500に記録して、この記録媒体500に記録されたプログラムを同図に示したコンピュータ400に読み込ませ、実行することにより各機能を実現してもよい。

【0204】

同図に示したコンピュータ400は、上記プログラムを実行するCPU410と、キーボード、マウス等の入力装置420と、各種データを記憶するROM430と、演算パラメータ等を記憶するRAM440と、記録媒体500からプログラムを読み取る読取装置450と、ディスプレイ、プリンタ等の出力装置460と、装置各部を接続するバス470とから構成されている。

【0205】

CPU410は、読取装置450を経由して記録媒体500に記録されているプログラムを読み込んだ後、プログラムを実行することにより、前述した機能を実現する。なお、記録媒体500としては、光ディスク、フレキシブルディスク、ハードディスク等が挙げられる。

【0206】

(付記1) 情報を再生する情報再生装置において、

内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、

外部から参照することが可能なメモリと、

前記セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスにより前記メモリに格納されたメモリ格納情報を読み出し、該メモリ格納情報と、前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック手段と、

を備えたことを特徴とする情報再生装置。

【0207】

(付記 2) 前記改ざんチェック手段は、前記メモリ格納情報の全てを読み出すことを特徴とする付記 1 に記載の情報再生装置。

【 0 2 0 8 】

(付記 3) 前記改ざんチェック手段は、前記メモリ格納情報の一部を読み出すことを特徴とする付記 1 に記載の情報再生装置。

【 0 2 0 9 】

(付記 4) 前記改ざんチェック手段は、チェックサムにより前記メモリ格納情報と前記セキュアモジュール格納情報との比較を行うことを特徴とする付記 1 ～ 3 のいずれか一つに記載の情報再生装置。

【 0 2 1 0 】

(付記 5) 前記メモリ格納情報は、ソフトウェアであることを特徴とする付記 1 ～ 4 のいずれか一つに記載の情報再生装置。

【 0 2 1 1 】

(付記 6) 前記改ざんチェック手段は、不定期に前記メモリからの読み出しを行うことを特徴とする付記 1 ～ 5 のいずれか一つに記載の情報再生装置。

【 0 2 1 2 】

(付記 7) 前記セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスにより前記メモリに格納されたメモリ格納情報を書き換える書き換え手段を備え、前記改ざんチェック手段は、書き換え後のメモリ格納情報と前記セキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックすることを特徴とする付記 1 ～ 6 のいずれか一つに記載の情報再生装置。

【 0 2 1 3 】

(付記 8) 前記書き換え手段は、不定期に前記メモリ格納情報の書き換えを行うことを特徴とする付記 7 に記載の情報再生装置。

【 0 2 1 4 】

(付記 9) 前記書き換え手段は、前記メモリ格納情報の一部を書き換えることを特徴とする付記 7 または 8 に記載の情報再生装置。

【 0 2 1 5 】

（付記 1 0）前記セキュアモジュールに実装され、原情報に変更をかけ、変更後の情報をメモリ格納情報として前記メモリに格納する格納制御手段を備えたことを特徴とする付記 1 ～ 9 のいずれか一つに記載の情報再生装置。

【 0 2 1 6 】

（付記 1 1）前記格納制御手段は、前記メモリ格納情報を更新した場合に、更新前のメモリ格納情報から更新後のメモリ格納情報への引継を行わせることを特徴とする付記 1 0 に記載の情報再生装置。

【 0 2 1 7 】

（付記 1 2）前記格納制御手段は、前記セキュアモジュール内のみに存在する鍵を用いて前記原情報を暗号化し、暗号化された原情報を前記メモリ格納情報として前記メモリに格納することを特徴とする付記 1 0 または 1 1 に記載の情報再生装置。

【 0 2 1 8 】

（付記 1 3）前記セキュアモジュールに実装されており、前記メモリ格納情報の暗号化または復号化に用いられる鍵を保持し、前記改ざんチェック手段により改ざんが検知されない場合、鍵を外部へ供給する鍵管理手段を備えたことを特徴とする付記 1 ～ 1 2 のいずれか一つに記載の情報再生装置。

【 0 2 1 9 】

（付記 1 4）前記鍵管理手段は、有効時間が設定された前記鍵を供給することを特徴とする付記 1 3 に記載の情報再生装置。

【 0 2 2 0 】

（付記 1 5）前記鍵管理手段は、供給の度に鍵を変更することを特徴とする付記 1 3 または 1 4 に記載の情報再生装置。

【 0 2 2 1 】

（付記 1 6）前記鍵管理手段は、前記改ざんチェック手段により改ざんが検知された場合、前記鍵の供給を停止することを特徴とする付記 1 3 ～ 1 5 のいずれか一つに記載の情報再生装置。

【 0 2 2 2 】

（付記 1 7）前記セキュアモジュールに実装され、直接アクセスにより、前記セ

セキュアモジュール内の秘密情報を前記メモリに書き込む書込手段を備え、前記改ざんチェック手段は、書き込まれた前記秘密情報に対応する応答情報に基づいて前記メモリ格納情報の改ざんをチェックすることを特徴とする付記 1 ～ 1 6 のいずれか一つに記載の情報再生装置。

【 0 2 2 3 】

(付記 1 8) 前記秘密情報は、1 度目で正規の情報が読み出され 2 度目で違う情報が読み出されるように制御されるメモリ空間に格納されていることを特徴とする付記 1 7 に記載の情報再生装置。

【 0 2 2 4 】

(付記 1 9) 内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュール内で実行され、いずれの手段も介さずに直接アクセスにより外部から参照することが可能なメモリに格納されたメモリ格納情報を読み出す読み出し工程と、

読み出された前記メモリ格納情報と前記セキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、前記メモリ格納情報の改ざんをチェックする改ざんチェック工程と、

を備えたことを特徴とする情報再生方法。

【 0 2 2 5 】

【発明の効果】

以上説明したように、本発明によれば、いずれの手段も介さずに直接アクセスによりメモリに格納されたメモリ格納情報を読み出し、該メモリ格納情報とセキュアモジュールに予め格納されたセキュアモジュール格納情報との比較結果に基づいて、メモリ格納情報の改ざんをチェックすることとしたので、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェア（セキュアモジュール）を付加することで、安全なソフトウェア処理を実行することができるという効果を奏する。

【 0 2 2 6 】

また、本発明によれば、セキュアモジュールに実装され、いずれの手段も介さずに直接アクセスによりメモリに格納されたメモリ格納情報を書き換える書き換

え手段を設け、書き換え後のメモリ格納情報とセキュアモジュール格納情報との比較結果に基づいて、メモリ格納情報の改ざんをチェックすることとしたので、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェア（セキュアモジュール）を付加することで、安全なソフトウェア処理を実行することができるという効果を奏する。

【 0 2 2 7 】

また、本発明によれば、セキュアモジュールに実装され、原情報に変更をかけ、変更後の情報をメモリ格納情報としてメモリに格納することとしたので、さらに安全なセキュア環境を提供することができるという効果を奏する。

【 0 2 2 8 】

また、本発明によれば、メモリ格納情報を更新した場合に、更新前のメモリ格納情報から更新後のメモリ格納情報への引継を行わせることとしたので、更新に伴う処理停止を回避することができるという効果を奏する。

【 0 2 2 9 】

また、本発明によれば、セキュアモジュール内のみに存在する鍵を用いて原情報を暗号化し、暗号化された原情報をメモリ格納情報としてメモリに格納することとしたので、さらに安全なセキュア環境を提供することができるという効果を奏する。

【 0 2 3 0 】

また、本発明によれば、メモリ格納情報の暗号化または復号化に用いられる鍵を保持し、改ざんチェック手段により改ざんが検知されない場合、鍵を外部へ供給することとしたので、安全性が高い状態で暗号化または復号化を行うことができるという効果を奏する。

【 0 2 3 1 】

また、本発明によれば、改ざんチェック手段により改ざんが検知された場合、鍵の供給を停止することとしたので、改ざんによる損害を最小限にとどめることができるという効果を奏する。

【 0 2 3 2 】

また、本発明によれば、直接アクセスにより、セキュアモジュール内の秘密情

報をメモリに書き込む書込手段を備え、書き込まれた秘密情報に対応する応答情報に基づいてメモリ格納情報の改ざんをチェックすることとしたので、さらに安全なセキュア環境を提供することができるという効果を奏する。

【 0 2 3 3 】

また、本発明によれば、1度目で正規の情報が読み出され2度目で違う情報が読み出されるように制御されるメモリ空間に秘密情報を格納することとしたので、さらに安全なセキュア環境を提供することができるという効果を奏する。

【図面の簡単な説明】

【図 1】

本発明にかかる一実施の形態の構成を示すブロック図である。

【図 2】

図 1 に示したパーソナルコンピュータ 1 0 0 における電源投入時のセキュア機能を説明するブロック図である。

【図 3】

図 1 に示したパーソナルコンピュータ 1 0 0 における通常動作時のセキュア機能を説明するブロック図である。

【図 4】

図 1 に示したパーソナルコンピュータ 1 0 0 における全切替時のセキュア機能を説明するブロック図である。

【図 5】

図 1 に示したパーソナルコンピュータ 1 0 0 における一部切替時のセキュア機能を説明するブロック図である。

【図 6】

同一実施の形態の変形例の構成を示すブロック図である。

【図 7】

パーソナルコンピュータ 5 0 を用いた従来のシステムの構成例を示すブロック図である。

【図 8】

図 7 に示したパーソナルコンピュータ 5 0 における情報の流れを説明する図で

ある。

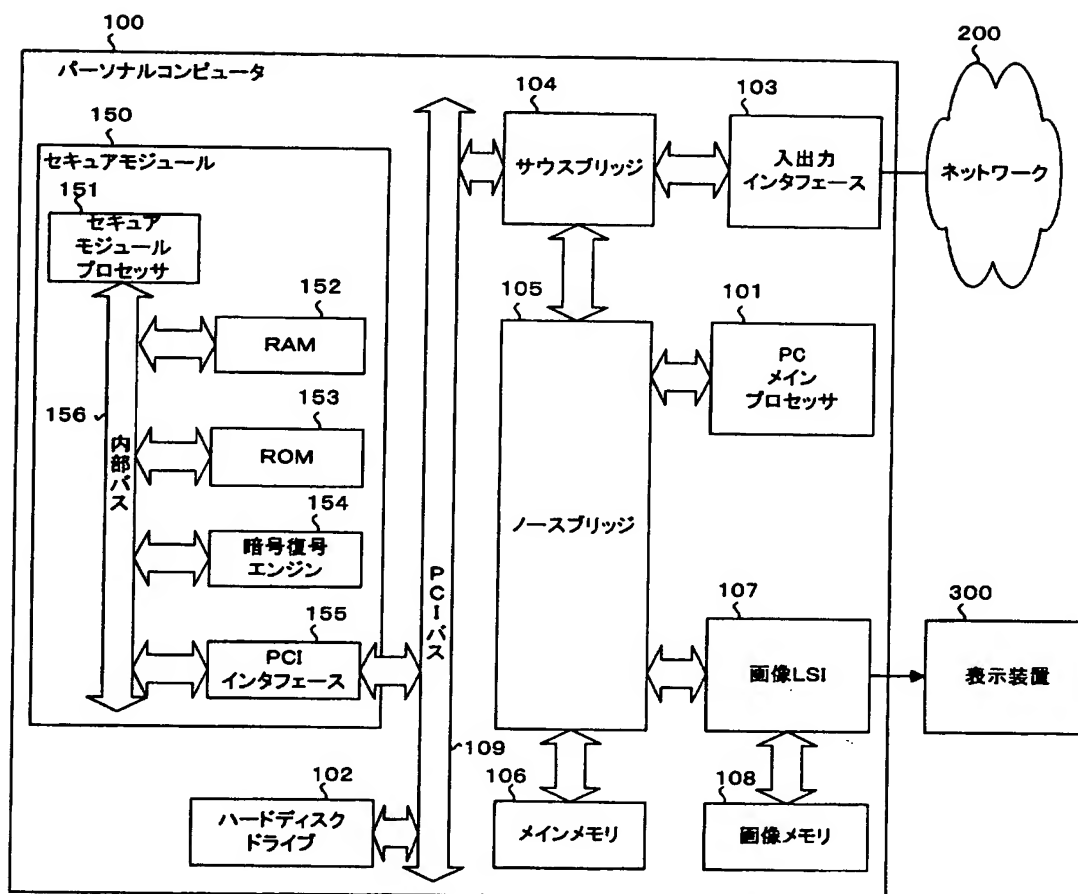
【符号の説明】

- 1 0 0 パーソナルコンピュータ
- 1 0 1 P C メインプロセッサ
- 1 0 2 ハードディスクドライブ
- 1 0 6 メインメモリ
- 1 0 7 画像 L S I
- 1 0 8 画像メモリ
- 1 0 9 P C I バス
- 1 5 0 セキュアモジュール
- 1 5 1 セキュアモジュールプロセッサ
- 1 5 2 R A M
- 1 5 3 R O M
- 1 5 4 暗号復号エンジン
- 1 5 5 P C I インタフェース
- 2 0 0 ネットワーク
- 3 0 0 表示装置
- 1 6 0 初期化／ロード部
- 1 7 0 ドライバ
- 1 8 0 セキュアソフトウェア
- 1 8 0' セキュアソフトウェア
- 1 8 1 入力バッファ
- 1 8 2 T S デコーダ
- 1 8 3 ビデオバッファ
- 1 8 4 暗号復号部
- 1 8 5 小バッファ
- 1 8 6 M P E G ビデオデコーダ
- 1 8 7 M P E G 画像メモリ
- 1 8 8 M P E G 出力部

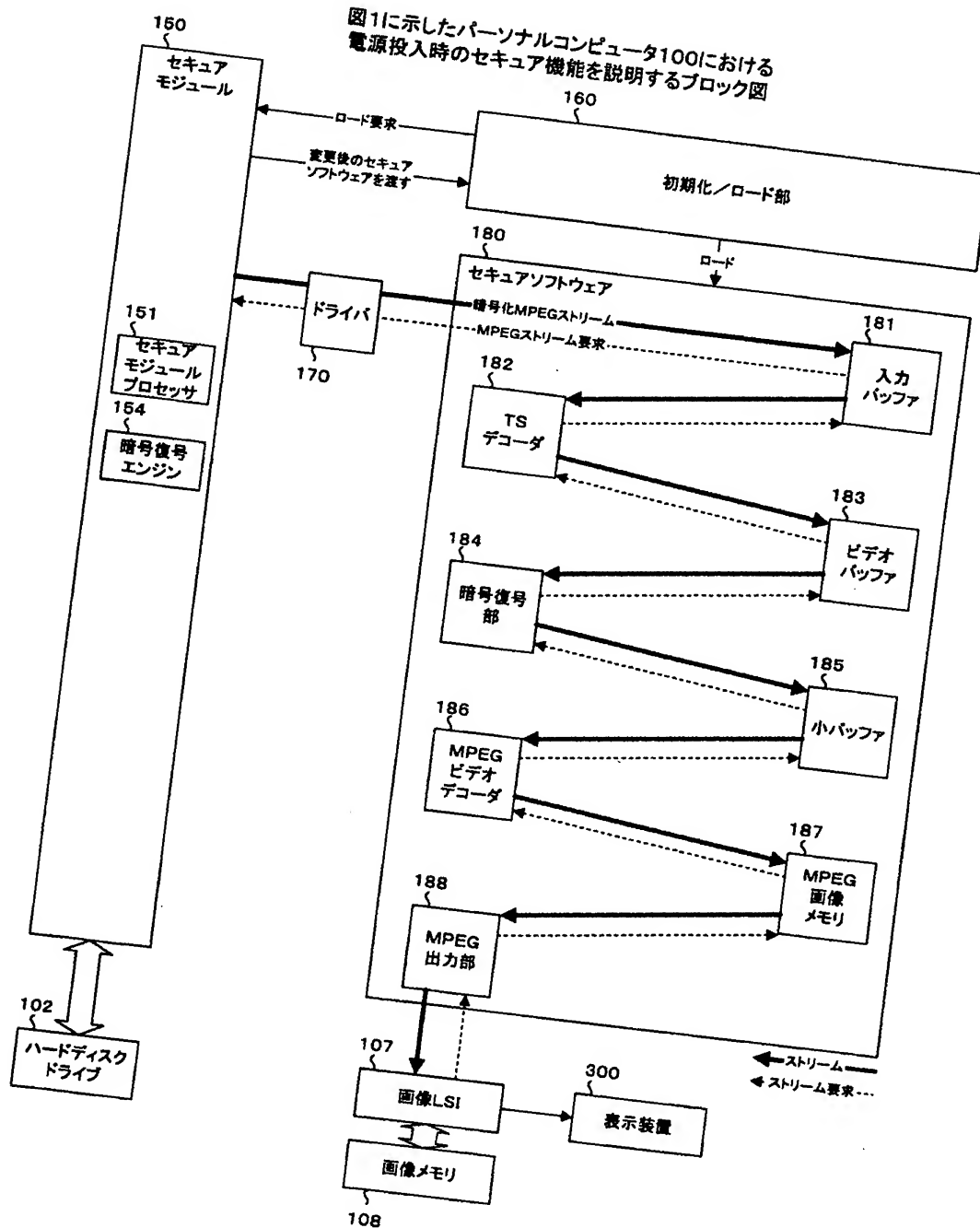
【書類名】 図面

【図 1】

一実施の形態の構成を示すブロック図

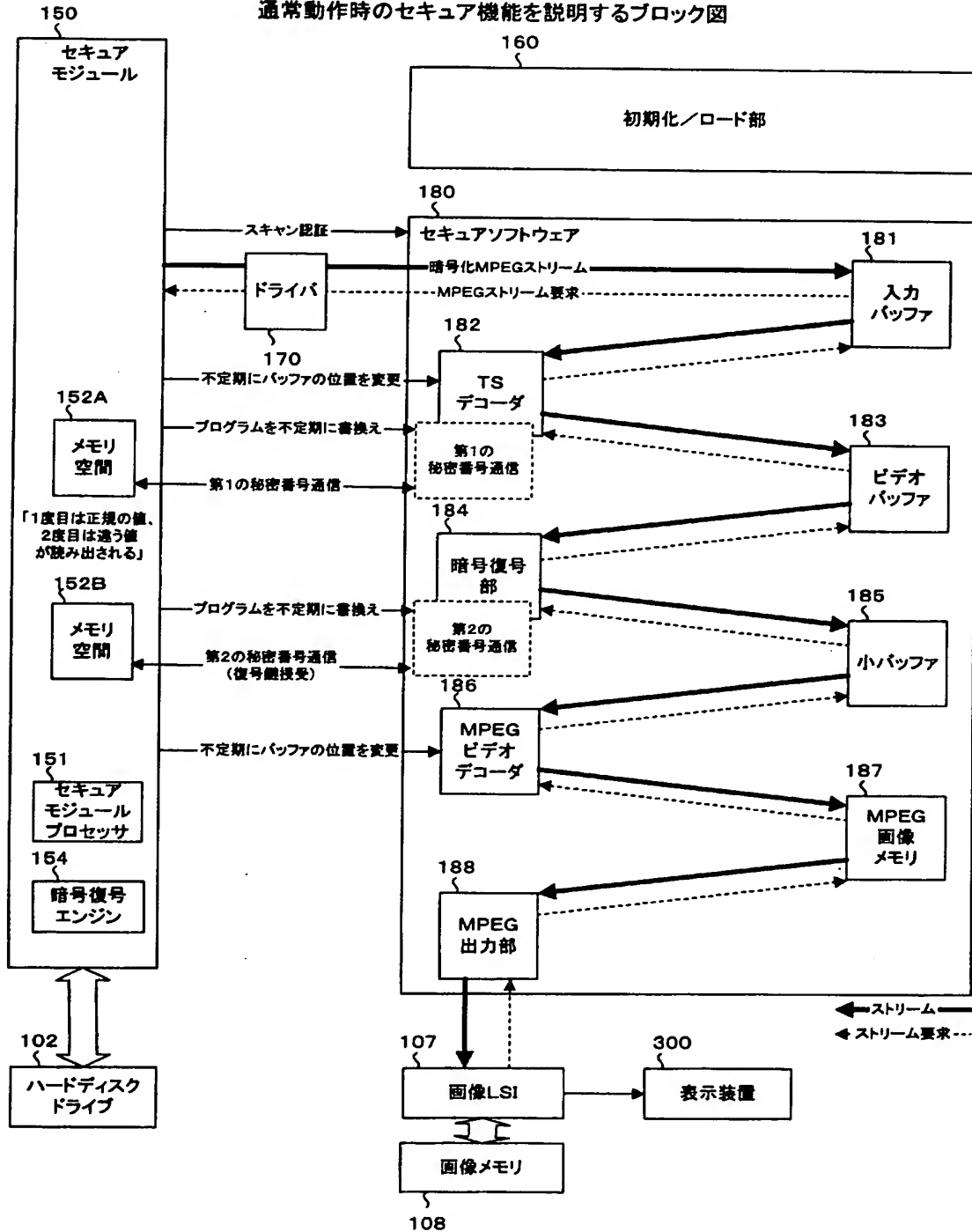


【図2】



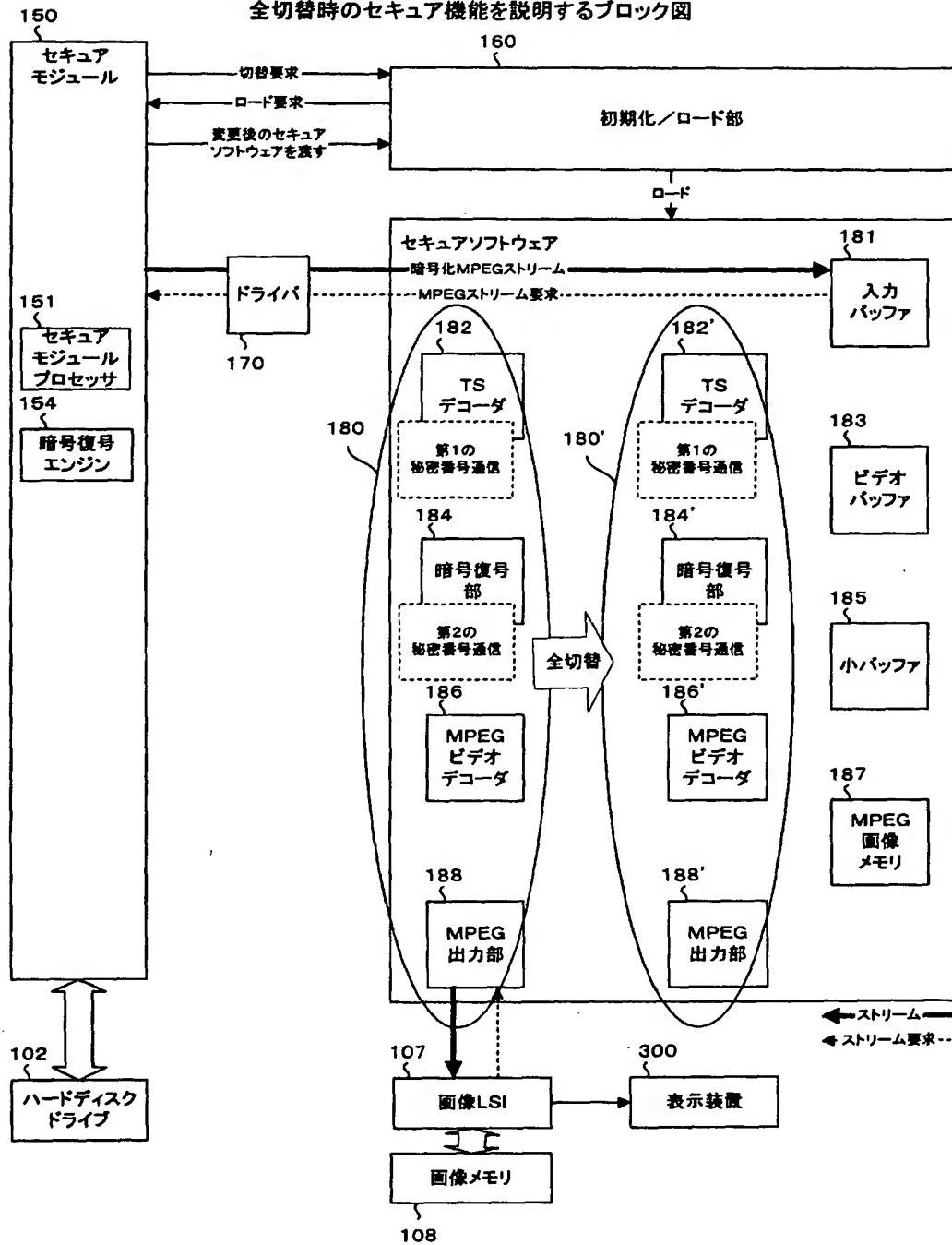
【図 3】

図1に示したパーソナルコンピュータ100における通常動作時のセキュア機能を説明するブロック図



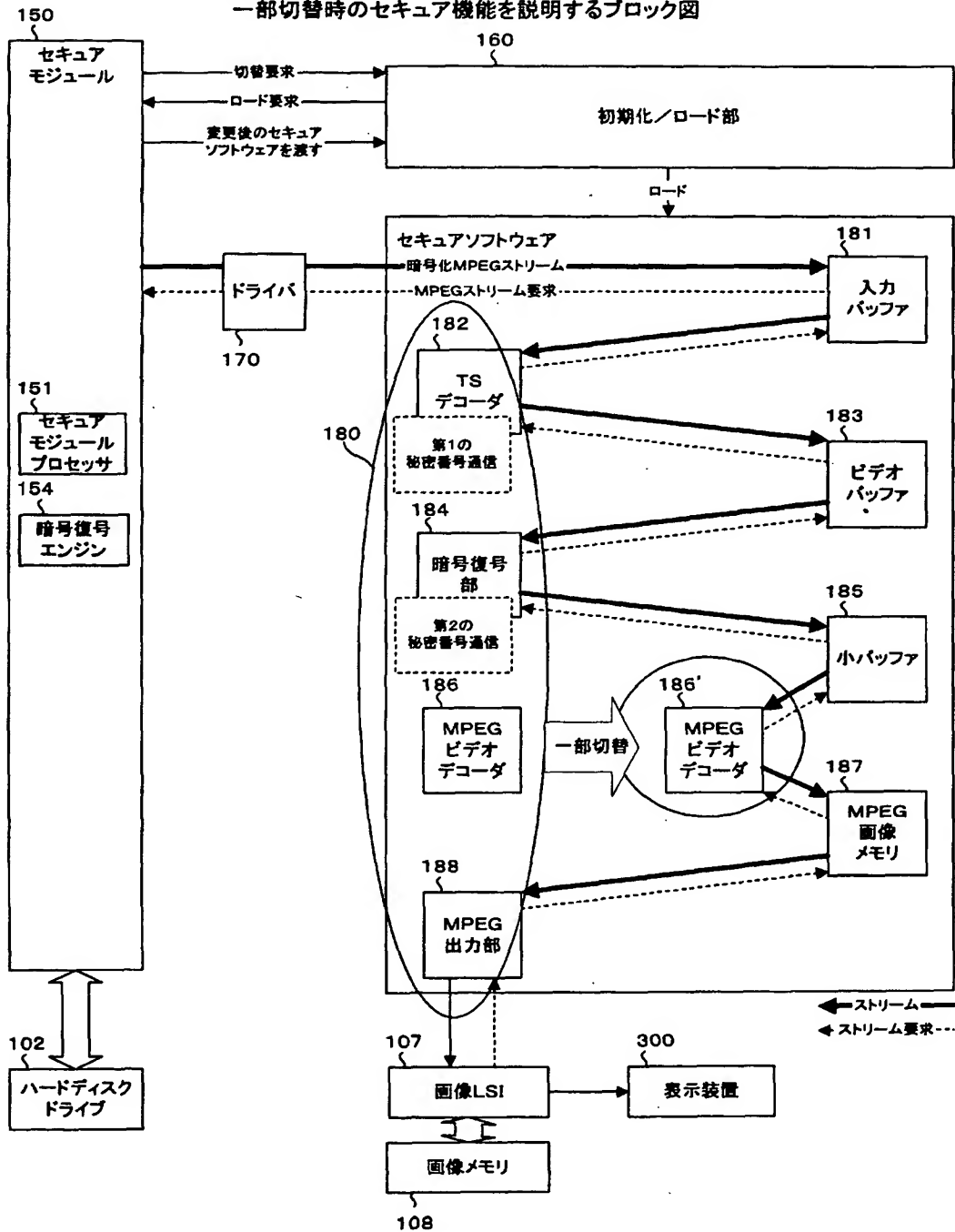
【図 4】

図1に示したパーソナルコンピュータ100における全切替時のセキュア機能を説明するブロック図



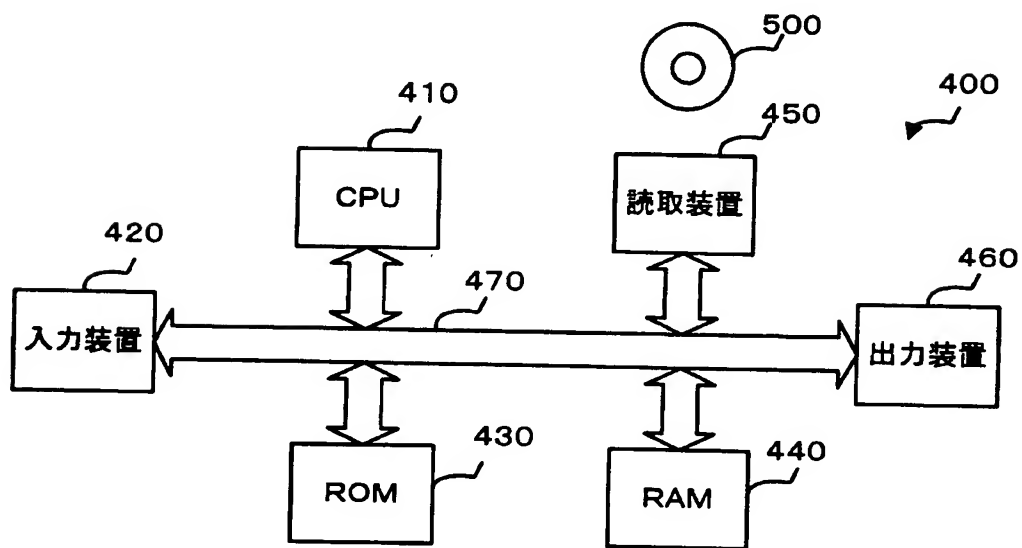
【図5】

図1に示したパーソナルコンピュータ100における
一部切替時のセキュア機能を説明するブロック図



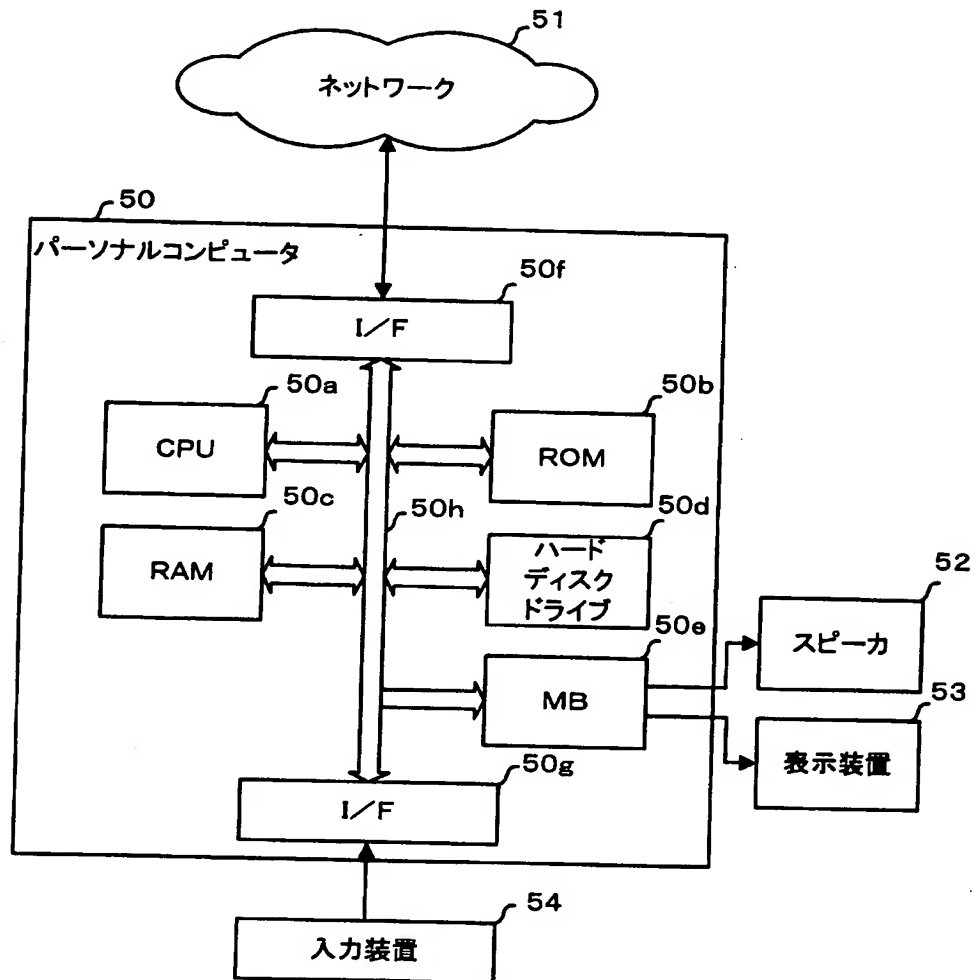
【図 6】

一実施の形態の変形例の構成を示すブロック図



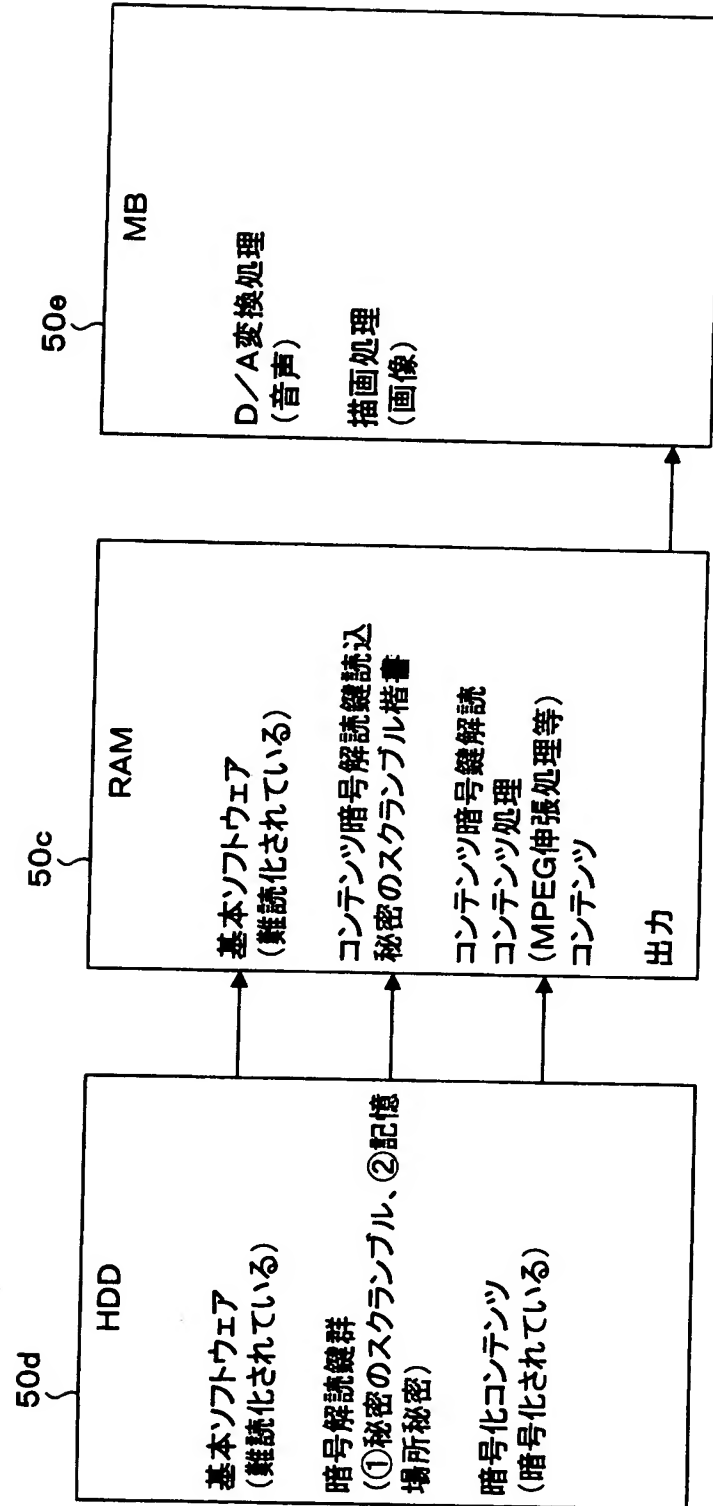
【図7】

パーソナルコンピュータ50を用いた従来のシステムの構成例を示すブロック図



【図 8】

図 7 に示したパーソナルコンピュータ 5 0 における情報の流れを説明する図



【書類名】 要約書

【要約】

【課題】 パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して、最低限のハードウェアを付加することで、安全なソフトウェア処理を実行させること。

【解決手段】 内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュール 1 5 0 と、外部から参照することが可能なメインメモリを備え、セキュアモジュール 1 5 0 は、いずれの手段も介さずに直接アクセスによりメインメモリに格納されたセキュアソフトウェア 1 8 0 のコード等を読み出し、このコード等と予め格納された情報との比較結果に基づいて、セキュアソフトウェア 1 8 0 の改ざんをチェックする。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号

[000005223]

1. 変更年月日

1996年 3月26日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中4丁目1番1号

氏 名

富士通株式会社